Special Topics on Applied Mathematical Logic

Spring 2012

Lecture 01

Jie-Hong Roland Jiang

National Taiwan University

February 24, 2012

Outline

What is logic?

- Logic is the study of deductive thoughts, just like probability is the study of uncertainty
- Logical deduction

$$\frac{\text{All men are mortal.}\qquad \text{Socrates is a man.}}{\text{Socrates is mortal.}} \qquad\qquad \frac{\forall x \in S. P(x) \qquad y \in S}{P(y)}$$

- Metamathematics (syntax, semantics, deduction)

Basic Facts about Sets

- A **set** is a collection of things, called its **members** or **elements**
  $t \in A$ — t is a member of A
  $t \notin A$ — t is not a member of A
  $x = y$ — x, y are the same object
- For $A = B$, we mean $t \in A$ iff $t \in B$. That is, a set is determined by its members.
- Adjoin an object to a set, denoted $A; t = A \cup \{t\}$, where t may or may not be a member of A. ($t \in A$ iff $A; t = A$)

Example Sets

- $\emptyset$ — empty set; with no members at all (in contrast to nonempty sets)
- $\{x\}$ — singleton set; with a single member

  $\vdots$
- $\{x_1, \ldots, x_n\}$

  $\vdots$
- Natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$
- Integers $\mathbb{Z} = \{\ldots, -1, 0, 1, \ldots\}$
- Note that $\{x, y\} = \{y, x\}$ (unordered)

Notation

- To define a set, we use the notation $\{x \mid \text{property of x}\}$

  E.g., $\{\langle m, n\rangle \mid m, n \in \mathbb{N}, m < n\}$

  $\{x \mid (x \text{ mod } 5) = 0, x \in \mathbb{N}\}$

Set Inclusion and Power Sets

- $A \subseteq B$ means $x \in A \Rightarrow x \in B$
- $A \subset B$ means $A \subseteq B$ and $\exists x(x \in B$ and $x \notin A)$
- $\emptyset$ is a subset of every set ($\emptyset \subseteq \emptyset$; also $\emptyset \subseteq A$ is vacuously true)
- Power set of A, denoted $\mathcal{P}A = \{x \mid x \subseteq A\}$
  E.g., $\mathcal{P}\emptyset = \{\emptyset\}$
  $\mathcal{P}\{\emptyset\} = \{\emptyset, \{\emptyset\}\}$
  $\mathcal{P}\{\emptyset, \{\emptyset\}\} = \{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}, \{\emptyset, \{\emptyset\}\}\}$
  $\vdots$

Set Operations

- Union: $A \cup B$
- Intersection: $A \cap B$
  Disjoint: $A \cap B = \emptyset$
  Pairwise disjoint: $A_i \cap A_j = \emptyset$, $i, j = 1, \ldots, n$, $i \neq j$
- (Big)union: $\bigcup A = \{x \mid x$ belongs to some member of $A\}$
- (Big)intersection: $\bigcap A = \{x \mid x$ belongs to all member of $A\}$
  E.g., for $A = \{\{0, 1, 5\}, \{1, 5\}, \{0, 2\}\}$,
  $\bigcup A = \{0, 1, 2, 5\}$
  $\bigcap A = \emptyset$
  $A \cup B = \bigcup\{A, B\}$, for any B
  $\bigcup \mathcal{P}A = A$

Ordered Sets

- Ordered pair $\langle x, y\rangle$ of objects x and y must be defined such that $\langle x, y\rangle = \langle u, v\rangle$ iff $x = u$ and $y = v$
  E.g., define $\langle x, y\rangle$ as $\{x, \{x, y\}\}$ (so the order is distinguished)
- Recursive generalization of $\langle x, y\rangle$ to n-tuples:

$$\begin{aligned} \langle x, y, z\rangle &\triangleq \langle\langle x, y\rangle, z\rangle \\ &\vdots \\ \langle x_1, \ldots, x_{n+1}\rangle &\triangleq \langle\langle x_1, \ldots, x_n\rangle, x_{n+1}\rangle \end{aligned} \tag{1}$$

  Eq. (1) holds for $n \geq 1$ by letting $\langle x\rangle \triangleq x$
- Cartesian product $A \times B = \{\langle x, y\rangle \mid x \in A, y \in B\}$ and $A^n = \{\langle x_1, \ldots, x_n\rangle \mid x_i \in A, i = 1, \ldots, n\}$

Finite Sequences

- S is a **finite sequence** (or **string**) of members of A iff $S = \langle x_1, \ldots, x_n\rangle$, where every $x_i \in A$ for $n \in \mathbb{Z}^+$
- A **segment** of the finite sequence $S = \langle x_1, \ldots, x_n\rangle$ is a finite sequence $\langle x_k, x_{k+1}, \ldots, x_{m-1}, x_m\rangle$ with $1 \leq k \leq m \leq n$
- If $\langle x_1, \ldots, x_n\rangle = \langle y_1, \ldots, y_n\rangle$, then $x_i = y_i$ for $i = 1, \ldots, n$

What if $\langle x_1, \ldots, x_m\rangle = \langle y_1, \ldots, y_n\rangle$ and $m \neq n$?

Sequences of Different Lengths

Lemma

If $\langle x_1, \ldots, x_m \rangle = \langle y_1, \ldots, y_{m+k} \rangle$*, then* $x_1 = \langle y_1, \ldots, y_{k+1} \rangle$ *for* $i = 1, \ldots, n$

Prove by induction on m with the observation that $\langle x, y, z \rangle = \langle \langle x, y \rangle, z \rangle$

Relations

- A **relation** R is a set of ordered pairs
  E.g.,
  $R = \{\langle x, y \rangle \mid x < y, x, y = 0, 1, 2\} = \{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 1, 2 \rangle\}$
- The **domain** of R, denoted dom R, is the set $\{x \mid \langle x, y \rangle \in R \text{ for some } y\}$
- The **range** of R, denoted ran R, is the set $\{y \mid \langle x, y \rangle \in R \text{ for some } x\}$
- The **field** of R, denoted fld R, is the set $\mathrm{dom} R \cup \mathrm{ran} R$
- An n-**ary relation** on A is a subset of A^n
  What if $n = 1$? (just a subset of A)
- Let $R \subseteq A^n$. Then the **restriction** of R to B is $R \cap B^n$
  E.g., $\{\langle 0, 1 \rangle, \langle 0, 2 \rangle, \langle 1, 2 \rangle\} = \{\langle x, y \rangle \mid x < y, x, y \in \mathbb{N}\} \cap \{0, 1, 2\}^2$

Functions

- A **function** F is a relation being *single-valued*, i.e., for every $x \in \mathrm{dom} F$ if $\langle x, y_1 \rangle \in F$ and $\langle x, y_2 \rangle \in F$, then $y_1 = y_2$ (We denote such unique y as $F(x)$)
- A function defines some mapping $F : A \to B$
  $\mathrm{dom} F = A$, $\mathrm{ran} F \subseteq B$ (B is called the **co-domain** of F)
- If $\mathrm{ran} F = B$, then F maps A **onto** B (surjective)
- F is **one-to-one** iff, for every $y \in \mathrm{ran} F$, there is only one x s.t. $\langle x, y \rangle \in F$
- As notational convention, $F(x_1, \ldots, x_n)$ is meant to be $F(\langle x_1, \ldots, x_n \rangle)$

Operation

- An ***n*-ary operation** on A is a function $f : A^n \to A$
  E.g., $+ : \mathbb{N}^2 \to \mathbb{N}$; successor function $S : \mathbb{N} \to \mathbb{N}$
- The **restriction** of an n-ary operation f on A to a subset $B \subseteq A$ is the n-ary operation $g : B^n \to A$ with $g = f \cap (B^n \times A)$
- $\{\langle x, x \rangle \mid x \in A\}$ is the **identity function** Id on A, i.e., $\mathrm{Id}(x) = x$

Equivalence Relations

- For a relation R,
  - R is **reflexive** on A iff $\langle x, x \rangle \in R$ for every $x \in A$
  - R is **symmetric** on A iff $\langle x, y \rangle \in R$ implies $\langle y, x \rangle \in R$
  - R is **transitive** on A iff $\langle x, y \rangle \in R$ and $\langle y, z \rangle \in R$ imply $\langle x, z \rangle \in R$
- R is an **equivalence relation** on A iff R is a binary relation on A that is reflexive, symmetric, and transitive
- For an equivalence relation, its **equivalence classes** form a **partition** on A (i.e., each $x \in A$ belongs to exactly one equivalence class). The equivalence class of x is denoted $[x] = \{y \mid \langle x, y \rangle \in R\}$.

Ordering Relations

- R satisfies **trichotomy** on A iff for every $x, y \in A$ exactly one of the three possibilities, $\langle x, y \rangle \in R$, $x = y$, or $\langle y, x \rangle \in R$, holds
- R is an **ordering relation** on A iff R is transitive and satisfies trichotomy on A
  E.g.,

$$< \text{ on } \mathbb{N} \text{ is an ordering relation}$$

$$\text{how about } \leq \text{ on } \mathbb{N}?$$

Finite vs. Infinite Sets

- A set A is **finite** iff there is some one-to-one function f mapping A *onto* $\{0, 1, \ldots, n-1\}$ for some $n \in \mathbb{N}$
- A set A is **countable** iff there is some function f one-to-one into $\mathbb{N}$
  E.g., any finite set is countable
  - $\mathbb{N} \cup \{x\}$ is countable
  - $\mathbb{Z}$ is countable
  - $\mathbb{Q}$ is countable
  - $\mathbb{N} \times \cdots \times \mathbb{N}$ is countable
  - $(0, 1]$ is not countable
  - $\mathbb{R}$ is not countable
  - $\mathcal{P}\mathbb{N}$ is not countable
  - $\mathbb{N} \times \mathbb{N} \times \cdots$ is not countable

Countable vs. Uncountable

- $\mathbb{Q}$ is countable?
- $(0, 1]$ is uncountable?

Lemma
The union of countably many countable sets is countable

Lemma
The Cartesian product of infinitely many of $\{0, 1\}$ is not countable

Trees

$\{c\}$
0

$\{a, b, c, e\}$
5

$\{a\}$
2

root
$\{a, b, c, d, e\}$
7

$\{a, b, e\}$
4

$\{a, e\}$
3

$\{a, b\}$
6

$\{e\}$
1

A tree grows downward.

Chains

- A collection C of sets is a **chain** iff for any elements x and y of C, either $x \subseteq y$ or $y \subseteq x$
  E.g., tree with containment relation (transitive)

Lemma (Zorn's Lemma)

Suppose A is a set s.t., for any chain $C \subseteq A$, $\bigcup C \in A$. Then there is some $m \in A$ which is maximal (not a subset of any other element of A)

(an equivalent statement of the *axiom of choice*)

Cardinal Numbers

- A and B are **equinumerous**, denoted $A \sim B$, iff there is a *bijection* (one-to-one and onto mapping) between A and B
- $\sim$ is reflexive, symmetric, and transitive, i.e., an equivalence relation
- Two sets A and B are assigned the same **cardinal number** (or **cardinality**) iff they are equinumerous. That is,

  $$\mathrm{card} A = \mathrm{card} B \Leftrightarrow A \sim B$$

  (think of card as some abstract object)
- A is **dominated** by B, denoted $A \preccurlyeq B$, iff A is equinumerous with a subset of B. That is,

  $$\mathrm{card} A \leq \mathrm{card} B \Leftrightarrow A \preccurlyeq B$$

- Dominance relation is reflexive and transitive

Cardinal Numbers

Theorem (Schröder-Bernstein Theorem)

(a) *For any sets A and B, if $A \preccurlyeq B$ and $B \preccurlyeq A$, then $A \sim B$*

(b) *For any cardinal numbers κ and λ, if $\kappa \leq \lambda$ and $\lambda \leq \kappa$, then $\kappa = \lambda$*

Theorem

(a) *For any sets A and B, either $A \preccurlyeq B$ or $B \preccurlyeq A$*

(b) *For any cardinal numbers κ and λ, either $\kappa \leq \lambda$ or $\lambda \leq \kappa$*

Cardinal Numbers

$0, 1, 2, \ldots, \aleph_0, \aleph_1, \aleph_2, \ldots$

- $\aleph_0 = \mathrm{card}\mathbb{N}$ (the first infinite cardinal)
- $\aleph_1 = \mathrm{card}\mathbb{R} = 2^{\aleph_0}$ under CH (Continuum Hypothesis — $\nexists S.\mathrm{card}\mathbb{N} < |S| < \mathrm{card}\mathbb{R}$)
- Recall $\mathrm{card}\mathbb{R} > \mathrm{card}\mathbb{N}$

Cardinal Arithmetics

- For two disjoint sets A and B with cardinalities κ and λ, respectively, then $\kappa + \lambda = \mathrm{card}(A \cup B)$ and $\kappa \cdot \lambda = \mathrm{card}(A \times B)$

Theorem (Cardinal Arithmetic Theorem)

For cardinal numbers κ and λ, if $\kappa \leq \lambda$ and λ is infinite, then $\kappa + \lambda = \lambda$. Furthermore, if $\kappa \neq 0$, then $\kappa \cdot \lambda = \lambda$.

Theorem

For an infinite set A, $\mathrm{card} \bigcup_n A^{n+1} = \mathrm{card}A$